Safe-com

Babylon Familie

Broschüre

Babylon Familie

Oktober 2004

Version: 2.0

Inhaltsverzeichnis

1 Einführung

Die moderne Geschäftswelt ist ohne den Einsatz von Telekommunikation praktisch undenkbar. Unternehmen jeder Größe tauschen vertrauliche Informationen über offene Netzwerke wie Telefon-, Daten- und Internet-Verbindungen aus.

Verschlüsselungsplattform für Kommunikationsverbindungen

Allerdings sind öffentliche Netze angreifbar. Hacker und Wirtschaftsspione können sich Zugriff auf interne Informationen verschaffen, Gespräche abhören, den Datenaustausch auffangen und missbrauchen.
Eine Abwehrmaßnahme gegen die Spionagegefahr ist der Einsatz starker Verschlüsselung, die Informationen vor fremdem Zugriff schützt. Safe-com hat sich auf dieses Thema spezialisiert und entwickelte die Gerätefamilie Safe-com Babylon.
Das Einsatzgebiet eines Safe-com Babylon ist die Verschlüsselung von Audio-, Video- und Datenkommunikation.

2 Stärkste Verschlüsselungsverfahren

Verschlüsselung schützt Datenpakete auf dem Weg über öffentliche Kommunikationsleitungen. Safe-com Babylon setzt dabei ausschließlich auf anerkannte Kryptografie-Standards wie Triple-DES und AES. Diese Verfahren übersetzen die Daten in einen geheimen Code. Im Gegensatz zur Verwendung proprietärer Verschlüsselungsalgorithmen hängt dabei die Sicherheit einzig von der Geheimhaltung der verwendeten Schlüssel ab. Bildlich gesprochen stecken Sie Ihre vertraulichen Daten mit Safe-com Babylon in einen sicheren Tresor und schließen ihn ab. Ist der Empfänger Ihrer Nachricht ebenfalls mit einem Babylon ausgestattet, so benötigt er nur noch den passenden Schlüssel, um Ihre Daten zu dechiffrieren. Ein Spion, der den Schlüssel nicht kennt, hat keine Chance, an Ihre Informationen zu gelangen.

Anerkannte Verschlüsselungsstandards

3 Sicherer Schlüsselaustausch

Auch beim Schlüsselaustausch setzt Safe-com Babylon auf internationale Standards. Neben der Möglichkeit, vom Sicherheitsbeauftragten feste Schlüssel vergeben zu lassen bietet Safe-com Babylon zwei dynamische Schlüsselaustauschprotokolle. Für jede neue Verbindung können Safe-com Babylon Geräte automatisch einen neuen Schlüssel generieren und über die Algorithmen Diffie-Hellman oder MDI (Master DES Internal)[1] austauschen. Selbstverständlich können die dynamischen Austauschverfahren

durch Authentisierungsmechanismen gegen aktive Angreifer - die so genannte 'Man-in-the-Middle-Attacke' - geschützt werden.

4 Vorteile der Babylon Produktfamilie

Die Babylon-Produktfamilie verschlüsselt die Kommunikationsdaten auf der Übertragungsebene. Anders als "Anwendungen", wie Videokonferenz- oder E-Mail-Systeme, die eine eingebaute Verschlüsselung anbieten, gewährleistet die Babylon-Produktfamilie eine vollständige Unabhängigkeit zwischen der Netz-Infrastruktur und den Anwendungen, die sie benutzen. Ändert sich zum Beispiel das Videokonferenzsystem, muss man nicht auch das Verschlüsselungssystem ändern. Die Babylonprodukte zeichnen sich vor allem durch folgende Merkmale aus

Nahtlos zwischen privatem und öffentlichem Netz für Wähl- und Standleitungen einsetzbar - vollständig transparent für den Benutzer

- Erfüllung höchster Anforderungen an die Verschlüsselungsstärke
- Transparenz für den Anwender
- Umfangreiche Administrationsunterstützung durch den Safe-com SecurityManager
- Niedrige Betriebskosten durch Fernwartung und einfaches Gerätemanagement
- Breites Spektrum an verschlüsselbaren Übertragungsarten (ISDN, Frame Relay, X.25, Link-HDLC, Link-Bitstream, Inmarsat ISDN (M4/Fleet/GAN), Inmarsat B, IP)
- Standardkonformität der Sicherheitsmechanismen
- Skalierbarkeit und Einsatz unterschiedlicher Varianten in die selbe Kommunikationsinfrastruktur

5 Produkte der Babylon-Familie

Die Babylon Produkt-Familie besteht aus verschiedenen Varianten, die unterschiedliche Übertragungsprotokolle unterstützen.

5.1 Babylon ISDN

Babylon ISDN ist eine weltweit etablierte Verschlüsselungslösung für öffentliche ISDN-Netze. Sie bietet Schutz für Telefongespräche, Daten, Fax und Videokonferenzen. Sie

1. MDI ist der von Safe-com vergebene Name für ein standardisiertes Verfahren zum Sitzungsschlüsselaustausch (Industriestandard ISO/IEC 11770-2).

ist kompatibel mit allen auf ISDN basierenden Telefon-, Fax- und Videokonferenzsystemen.
Babylon ISDN unterstützt sowohl Euro-ISDN als auch internationale ISDN-Standards. Die Installation ist einfach. Um Telefonate, Faxe und Videokonferenzen zu schützen, wird das Gerät vor der TK-Anlage oder den ISDN-Endgeräten platziert. Babylon ISDN ist dabei sogar in der Lage, Sprachverbindungen über komprimierte Strecken störungsfrei zu verschlüsseln.
Safe-com Babylon ISDN Geräte sind in vier Varianten lieferbar

5.1.1 Safe-com Babylon PRI

Safe-com Babylon PRI (Primary Rate Interface) kann bis zu 30 B-Kanäle (USA: 23) mit einer maximalen Geschwindigkeit von 2 Mbps gleichzeitig verschlüsseln. Deshalb ist es ideal für die Absicherung der ISDN Kommunikation großer Unternehmen.
Die Lizenzvariante G.703 dient speziell der Absicherung von ISDN-Standleitungen. Ein besonderes Merkmal ist hierbei der 'Channelized'-Modus, in dem auch einzelne Kanäle als Standleitung ausgewählt werden können.

5.1.2 Safe-com Babylon 4xBRI

Safe-com Babylon 4xBRI (Basic Rate Interface) ist zur Verschlüsselung von bis zu vier ISDN S0-Anschlüssen lizenzierbar. Die maximale Übertragungskapazität liegt daher bei 512 kbps. Es ist daher besonders gut für kleine Büros oder Videokonferenzen geeignet.

5.1.3 Safe-com Babylon Basic

Safe-com Babylon Basic ist eine günstige Alternative zu Safe-com Babylon 4xBRI, wenn nur ein ISDN S0-Anschluß benötigt wird, z.B. für den sicheren Betrieb eines Heimarbeitsplatzes.

5.1.4 Safe-com Babylon SAT

Safe-com Babylon SAT verschlüsselt Satellitenkommunikation, die über die Dienste Inmarsat ISDN (M4/Fleet/GAN) und Inmarsat B (Highspeed) angeboten wird. Damit bietet Safe-com auch Sicherheit an Orten, an denen keine ausreichende Festnetz-Infrastruktur gegeben ist, z.B. auf Schiffen, Ölplattformen oder für Anwender, die häufig den Ort wechseln.

Alle ISDN-Modelle unterstützen das Verschlüsselungsverfahren Triple-DES mit einer Schlüssellänge von 192 Bit. Die Modelle Babylon 4xBRI, Basic und SAT unterstützen zusätzlich den Verschlüsselungsalgorithmus AES mit einer Schlüssellänge von bis zu 256 Bit.

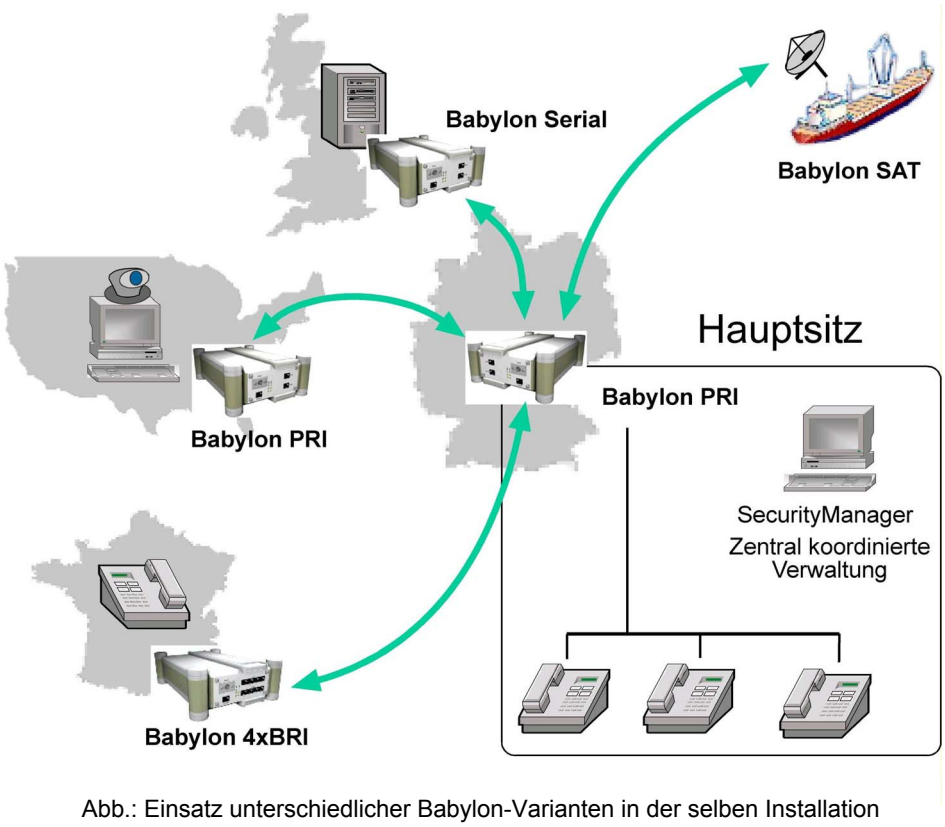

Abb.: Einsatz unterschiedlicher Babylon-Varianten in der selben Installation

5.2 Safe-com Babylon Serial

Safe-com Babylon Serial ist eine Verschlüsselungslösung für Netzwerke, die serielle Datenleitungen nutzen. Safe-com Babylon Serial unterstützt Verschlüsselung bei einer Netzwerkgeschwindigkeit von bis zu 2 Mbps.
Die Verbindungsmöglichkeiten basieren auf den Protokollen Link-HDLC, Frame Relay und X.25. Bei entsprechender Konfiguration kann Safe-com Babylon Serial auch den kompletten Datenstrom protokollunabhängig im Modus Link-Bitstream verschlüsseln. Ein besonderes Merkmal ist, dass auch ein ISDN-Babylon ein serielles Babylon im Bitstream-Modus als Gegenstelle haben kann. Die verschiedenen Übertragungsprotokolle sind einfach per Lizensierung auswählbar. Alle Varianten von Babylon Serial unterstützen Triple-DES mit einer Geschwindigkeit von bis zu 2Mbps. Die Variante Link-Bitstream unterstützt mit einer Geschwindigkeit von bis zu 384 kbps zusätzlich AES.

Babylon ISDN und Babylon Serial verfügen über SNMP- und Syslog-Funktionalität. Dadurch lassen sich alle Verbindungen in Echtzeit protokollieren.

5.3 Safe-com Babylon Giga

Safe-com Babylon Giga ist das erste in Deutschland entwickelte Verschlüsselungsgerät für Gigabit Ethernet. Babylon Giga unterstützt einen Durchsatz von 1 Gbit/s bei einer Latenzzeit von weniger als 50 Mikrosekunden. In der ersten Version verschlüsselt Babylon Giga Punkt-zu-Punkt-Verbindungen mittels Triple-DES mit einer Schlüssellänge von 192 Bit. Durch die Bereitstellung einer Krypto-API besteht für den Anwender auch die Möglichkeit, alternative Verschlüsselungsverfahren individuell zu implementieren. Zum Aufbau einer sicheren Verbindung verwendet Babylon Giga ein an den Internet Key Exchange (IKE) angelehntes Protokoll. Die Schlüssel werden hierbei über das Diffie-Hellman-Verfahren (1024 Bit) ausgetauscht.
Babylon Giga findet vor allem Anwendung in der Verschlüsselung des Datenverkehrs von 'Server Farms' und Backbones über MAN (Metropolitan Area Network), sowie WAN-Strecken, welche vor allem von großen Banken, multinationalen Unternehmen und international organisierten Behörden eingesetzt werden.

5.4 Safe-com Babylon IP

Safe-com Babylon IP sichert IP-basierte Videokonferenzen. Mit einem Durchsatz von bis zu 7 Mbps erfüllt Safe-com Babylon IP auch die höchsten Qualitätsansprüche an eine verschlüsselte Videokonferenz. Safe-com Babylon IP verzichtet konsequent auf jeglichen Einbau drehender Teile und Lüfter und arbeitet absolut geräuschlos. Daher ist Safe-com Babylon IP ideal für den Einsatz an einer geräuschempfindlichen Videokonferenzanlage gerüstet. Safe-com Babylon IP steht aber auch für andere Anwendungen bereit, z.B. Voice over IP. Safe-com Babylon IP unterstützt u.a. die Verschlüsselungsverfahren Triple-DES (192 Bit) und AES (bis zu 256 Bit).

6 Kosten-effektive Verwaltung

6.1 Safe-com SecurityManager

Kosten sparende Verwaltung der Sicherheit

Safe-com SecurityManager ist ein leistungsfähiges Softwaretool zur Fernwartung, mit dem die Safe-com Babylon Geräte von einer zentralen Stelle aus betreut werden können. Autorisierten Administratoren ist es so z.B. möglich, Schlüssel zentral zu verwalten, Benutzergruppen anzulegen und komplette Installationen zu konfigurieren. Weiter bietet der SecurityManager umfangreiche Möglichkeiten, die Sicherheitsrichtlinien des Anwenders in die Tat umzusetzen, z.B. durch Rollentrennung von Netzwerk- und Schlüsselmanagement oder durch die optionale Einführung des Vier-Augen-Prinzips. Alle Verbindungen zwischen der Managementsoftware und den angeschlossenen Geräten sind selbstverständlich verschlüsselt. Der Safe-com SecurityManager vereint großen Funktionsumfang mit einfacher Bedienung. Dadurch trägt

der SecurityManager dazu bei, die Betriebskosten der Sicherheitslösung minimal zu halten.

6.2 Überwachungsoptionen

Mit den Geräten der Babylon-Produktfamilie wird zahlreiches Zubehör zur Verfügung gestellt, welches den Zustand der Übertragung in Echtzeit darstellt. So kann der Anwender jederzeit überprüfen, welche Kommunikation (Gespräch, Videokonferenz, Datenaustausch) über welche Kanäle in verschlüsselter Form stattfindet.

7 Interoperabilität

Die Firmen Tandberg und Sony haben nach eingehenden Tests die Kompatibilität ihrer Videokonferenzsysteme mit Safe-com Babylon schriftlich bestätigt.

8 BSI-Zulassung

Die Geräte Safe-com Babylon 4xBRI und Safe-com Babylon PRI sind vom BSI (Bundesamt für Sicherheit in der Informationstechnik) für die nationale Geheimhaltungsstufe VS-NfD zugelassen.

Safe-com GmbH & Co. KG
Burg Lichtenfels 1
D - 35104 Lichtenfels
Germany

Tel.: +49 (0) 6454 - 79 96 03
Fax.: +49 (0) 6454 - 79 96 05
www.safe-com.com